United States
Mission Control Center
(USMCC)

System Operators Guide (SOG)

30 November 2006

Version 1.0

System Operators Guide (SOG)
Approval Page

_____
Joseph Wagenhofer
SSAI Project Manager

_____
William Burkhart
SARSAT Operations Team Lead

_____
Ajay Mehta
SARSAT Program Manager

_____
Brian Little
IPD, ISSO

Table of Contents

Table

1.0 Scope

1.1 Identification

This document details the Operators Guide for the National Oceanic and Atmospheric (NOAA)/United States Mission Control Center (USMCC) for the Search and Rescue Satellite-Aided Tracking system (Sarsat) NOAA5023. It is essentially a compilation of the USMCC Standard Operating Procedures (SOPs) used by the USMCC duty Controllers to operate the USMCC.

1.2 Document Overview

The USMCC SOG provides information and detailed procedures for initiating, operating, monitoring, and shutting down the USMCC. The SOG also provides information for identifying/isolating a malfunctioning component in the USMCC.

1.3 System Overview

The main purpose of the USMCC is to process information from emergency beacons that are detected by satellites and processed by Local User Terminals (LUTs), and to relay results to appropriate Search and Rescue (SAR) authorities. The USMCC operates as part of the United States Sarsat Ground System which, in turn, is part of the international Cospas-Sarsat search and rescue satellite system.

The USMCC is operated by NOAA on behalf of the U.S. Department of Commerce. The system is located at the NOAA Satellite Operations Facility (NSOF) in Suitland, Maryland. The system consists of a series of Intel based servers that use the Windows Operating System (Windows 2000 and 2003) to perform specific function(s) and exchange processed information.

The USMCC Operational System consists of the following PC/Server Components:

DB1 RAID Box
MccDb1A (Primary SQL Database)
MccDb1B (Backup SQL Database)
MccProc1
MccCom1
MccDisplay
MccOps1

The following PCs are used by the Operational and Test Systems (and are referenced as part of the Operational system):

MccOps2
MccPrim (Primary Domain Controller)

MccSec (Backup Domain Controller)
MccFtp1
MccFtp2
MccLUTFtp1
MccLUTFtp2

The USMCC is mainly an event driven system that responds to regularly scheduled input data from US LUTs as well as periodic input from other Cospas-Sarsart MCCs. The USMCC also processes data based on regularly scheduled events such as creation of satellite pass schedules that are used to control data acquisition at the US LUTs.

The USMCC is designed to automatically monitor its own processing and provide information to a system log on the results of the monitoring. The log and alarm messages are displayed on the operator console for action by the duty controller, if required.

2.0 References

The following documents contain additional information about the USMCC and its operations:

• USMCC Baseline Source Document (BSD). *This document contains details about the software modules of the USMCC*

• C/S A.001, Cospas-Sarsat Data Distribution Plan. *This document defines validation, filtering and routing procedures for messages exchanged with other Cospas-Sarsat MCCs and SPOCs.*

• C/S A.002, Cospas-Sarsat Standard Interface Document. *This document defines message formats and communication standards that are used by Cospas-Sarsat MCCs forinternational data exchange*

• C/S A.003, Cospas-Sarsat System Monitoring and Reporting. *This document provides international system monitoring and reporting requirements for MCCs.*

• C/S A.005, Cospas-Sarsat Mission Control Center Performance Specification and Design Guidelines. *This document details the international specifications for MCCs.*

• USMCC Functional Description Document (FDD). *This document provides a brief summary of the major hardware components and software processes used by the United States Mission Control Center*.

• National Cospas-Sarsat Network Interface Specifications (NTS). *This document defines the message format for data exchange between the USMCC and its LUTs.*

• USMCC Functional Requirements Document (FRD). *This document outlines the*

essential requirements of the USMCC

• USMCC Operating Instructions (UOI). *This document provides a detailed description of the screen formats and functionality that are used by the USMCC Operator Interface subsystem*

• United States Mission Control Center (USMCC) National Rescue Coordination Center (RCC) and Search and Rescue Point of Contact (SPOC) Alert and Support Messages. *This document describes the format and content for messages that are sent to the national RCCs and SPOCs and international SPOCs.*

• Telemetry and Command Procedures (TCP). *This document contains guidance on handling spacecraft telemetry data and commanding procedures.*

• USMCC Standard Operating Procedures (SOPs). *These documents provided detailed instructions for operating the USMCC.*

3.0 USMCC Operation

3.1 USMCC Stop and Start Procedures

3.1.1 Operational System

Complete Power-down of the USMCC Operational System

a. Contact the Operations Supervisor and advise him of the situation.
b. Notify MCCs, RCCs and SPOCs of the outage of the MCC.
c. Request all users to save any pending changes on the MccPrim, MccSec and SQL Database PCs (e.g., MS Word files and the MccOperational database) and to close connections to these PCs, if time permits. The Operations Supervisor will decide if this is appropriate, considering the likely impact on users and the USMCC.
d. Shut down the PCs/Servers in the following order:

MccProc1 -------- (MccTest rack)
Stop the following Services:
OPS_ALRT
OPS_INTF
OPS_LMONSERVICE
OPS_SMONSERVICE
Shutdown the PC

MccCom1 -------- (MccOps rack)
Stop the following Services:
OPS_COMMPROCESS

OPS_FTPFORTELEMETRY
OPS_OCVTSERVICE
Shutdown the PC

LUTFtp1 ------- (MccLUT rack)
Stop the following Service:
OPS_LUTFtpRelay
TST_LUTFtpRelay
Shutdown the PC

LUTFtp2 ------- (MccLUT rack)
Stop the following Service:
OPS_LUTFtpRelay
TST_LUTFtpRelay
Shutdown the PC

***Note 1:** At this time, the following PCs may be shut down if required. For any PCs involving the Systems Engineer, the Operations Supervisor may decide to power it off instead, based on the status of the USMCC and the availability of the Systems Engineer.

LUTServIDS ------ (MccLUT rack) (Systems Engineer or power off)
LUTServMonitor ------ (MccLUT rack) (Systems Engineer or power off)

MCCFtp1 --------- (MccDMZ rack)
Stop the following Services:
OPS_FaxFtpRelay
OPS_WebFtpRelay
TST_FaxFtpRelay
Shutdown the PC
[**See Note **2****]

MCCFtp2 --------- (MccDMZ rack)
Stop the following Services:
OPS_FaxFtpRelay
TST_FaxFtpRelay
Shutdown the PC
[**See Note **3****]

MCCDisplay -------- (MccTest rack)
Stop the MapDisplay – click on the "X" in the upper right hand corner.
Stop the SAMS display – click on the "X" in the upper right hand corner.
From the "Start" button, shutdown the PC

MCCOps2 -------- (Controller Console)
Close each Operator Interface program

Save and close any open documents (e.g., the Morning Briefing).
Close all windows on the desktop
From the "Start" button, shutdown the PC

MCCOps1 -------- (Controller Console)

Close each Operator Interface program
Save and close any open documents (e.g., the Morning Briefing).
Close all windows on the desktop
From the "Start" button, shutdown the PC

MCCDb1B --------- (MccOps rack) (Systems Engineer)

Preface: Unless unavoidable, have a Network Administrator present or on the telephone for this procedure.

Determine if the SQL Database is running on MCCDb1A, as follows:

a) Log into MCCDb1B, go to Start, Programs, Administrative tools, Cluster Administrator.
b) Expand MCCDb1A by clicking the "**+**" next to the folder.
c) Highlight the **Active Groups** folder and check if **Cluster Group** and **Disk Group2** are present and say **online** in the state column. If so, then the SQL Database is running on MCCDb1A, proceed to 11).
d) Expand MCCDb1B by clicking "+" next to the folder.
e) Highlight the **Active Groups** folder and check if **Cluster Group** and **Disk Group2** are present and say **online** in the state column. If so, then the SQL Database is running on MccDb1B, proceed to 7).
f) Otherwise, the SQL Database is not running on either MCCDb1A or MCCDb1B. **Notify the Operations Supervisor** *(Network Administrator?)* **immediately**.
g) Switch the SQL Database from MCCDb1B to MCCDb1A:
h) With **Active Groups** highlighted on MCCDb1B, in the right pane, right click **Cluster Group** and select **Move Group**.
i) Go to the active resources folder under MCCDb1A and wait for all resources to come online.
j) Return to the **Active Groups** folder under MCCDb1B, right click **Disk Group2** and select **Move Group.**
k) Return to the active resources folder under MCCDb1A and wait for all resources to come online.
l) Shutdown MccDb1B, as follows:
m) Highlight MCCDb1B, right click, and select Pause Node
n) From the "Start" button, shutdown the PC

MCCDb1A --------- (MccOps rack) (Systems Engineer)

a) Log into MCCDb1A
b) From the "Start" button, shutdown the PC

***Note 2:** At this time, the following PCs may be shut down if required.

MCCMonitor --------- (MccDMZ rack) (Systems Engineer)
MCCIds ---------- (MccDMZ rack) (Systems Engineer)

MCCSec ---------- (MccTest rack) (Systems Engineer)
Shut down the PC

MCCPrim --------- (MccTest rack) (Systems Engineer)
Shut down the PC

WEBInside and WEBOutside Racks

***Note 2:** After the MCCFtp1 PC has been shut down, the following PCs may be shut down if required.

DC1 --------- (MccWeb Inside rack) (Web Engineer)
DC2 --------- (MccWeb Inside rack) (Web Engineer)
RGDB FTP --------- (MccWeb Outside rack) (Web Engineer)
WebSrv --- (MccWeb Outside rack) (Web Engineer)
WebSrvDev --- (MccWeb Outside rack) (Web Engineer)
RGDB Document Image Server --- (MccWeb Outside rack) (Web Engineer)
AppSrv --- (MccWeb Inside rack) (Web Engineer)
AppSrv2 --- (MccWeb Inside rack) (Web Engineer)
AppSrvDev --- (MccWeb Inside rack) (Web Engineer)
RGDB WS --- (MccWeb Inside rack) (Web Engineer)
NOAA IDS --- (MccWeb Inside rack) (Web Engineer)
MONITOR --- (MccWeb Inside rack) (Web Engineer)

***Note 3:** After the MCCFtp2 PC has been shut down, the following PCs may be shut down if required.

MccFtpIDs --------- (MccDMZ rack) (Systems Engineer)
MccFtpMonitor ------ (MccDMZ rack) (Systems Engineer)
FaxBack Server ------ (MccDMZ rack) (Systems Engineer)
MccArchive DB ------ (MccTest rack) (Systems Engineer)

3.1.2 Test System

The USMCC Test System consists of the following Components

Hardware:

DB2 RAID Box
MccDb2A (Primary SQL Database)
MccDb2B (Backup SQL Database)
MccProc2
MccCom2

The following PCs are used by the Operational and Test Systems, and are referenced as part of the operational system.

MccOps2
MccPrim (Primary Domain Controller)
MccSec (Backup Domain Controller)
MccFtp1
MccFtp2
MccLUTFtp1
MccLUTFtp2

Complete Power-down of the USMCC Test System

a) Contact the Operations Supervisor and advise him of the situation.
b) Request all users to save any pending changes on the SQL Database PCs (e.g., the Test Database) and to close connections to these PCs, if time permits. The Operations Supervisor will decide if this is appropriate, considering the likely impact on users and the USMCC.
c) Shut down the PCs/Servers in the following order:

MccProc2 (MccTest Rack)
Stop the following Services:
TST_ALRT
TST_INTF
TST_LMONSERVICE
TST_SMONSERVICE
From the "Start" button, shutdown the PC

MccCom2 (MccOPS Rack)
Stop the following Services:
TST_COMMPROCESS
TST_FTPFORTELEMETRY
TST_OCVTSERVICE
Shutdown the PC

MCCDb2B (MccTest Rack)
**** Use the same procedure as used for MccDb1B

MCCDb2A (MccTest Rack)
**** Use the same procedure as used for MccDb1A

Complete Power-up of the USMCC Operational System

MccPrim PC

MccSec PC --- Wait until MccPrim is completely up and functioning correctly.

MCCDb1A and MCCDb1B Servers ---- Wait until MccPrim is completely up and functioning correctly. * Power on the MCCDb1A first; make sure it is functioning correctly then power on MCCDb1B.

MccOps1
MccOps/2
MccDisplay
MccLUTFtp1
MccLUTFtp2
MccFtp1
MccFtp2
MccCom1
MccProc1
MCCIDS
MCCMonitor

Complete Power-up of the USMCC Test System

a) Power on the MCCDb2A & MCCDb2B Servers
   i) Power on the MccDb2A first; make sure it is functioning correctly, then power on MccDb2B.
b) Power on the **USMCC Test Subsystems**.
   i) MccCom2
   ii) MccProc2

3.2 Operating Procedures

3.2.1 Input and Output Procedures

3.2.1.1 Procedures to Identify and Resolve Communications Problems.

Communications to/from the USMCC are highly automated and involve different communications vendors. To the extent possible, communication monitoring software is used to identify potential communication failures. This involves sequence checks on incoming message numbers, time interval gaps on message exchange, and disposition/acknowledgment codes for transmitted messages. For detailed information on these procedures **(ref. SOP MCCCom01).** Communication failures with the USA LUTs can be identified by late or missing data checks **(ref SOP MCCLUT05)**.

3.2.1.2 Guidance on How to Establish a Communications Site and Enable Alert Data to be Automatically Routed to the Site.

Sending alert data to a new Communications site is an important task, and requires prior authorization by the Operations Supervisor. In some cases, the Operations Supervisor

will request prior approval from NOAA for this task by submitting an SCP. Once the change is authorized, the Operations Supervisor will request the Communications Specialist and/or others to implement this change. **(ref. SOP MCCCom02)**

3.2.1.3 Identify and Respond to Missing Messages from MCCs

For those MCCs that use sequenced message numbering on messages sent to the USMCC, the expected message number is compared with the actual message number to identify potential communication outages that resulted in missing messages. Significant communication outages, including monitoring of MCCs that do not use sequence numbers, is monitored by measuring the gap in time since the last message was received. **(ref. SOP MCCCom03)**

3.2.1.4 Restarting the Communication Process

During reconfiguration of the USMCC communication subsystem, it is occasionally necessary to restart the communications process in order to load new values from the database into the registry. This procedure provides instructions for restarting the communication process.

Procedure: *Comm Process Restart*

a) To stop/start the Comm process, proceed to the PC that *currently* houses the Operational Communications Process, i.e., the MCCCOM1 PC or the MCCCOM2 PC.

b) Proceed to the Control Panel;
   Services;
   Stop 'OPS_COMMPROCESS';
   WAIT 20 SECONDS! ---
   Start 'OPS_COMMPROCESS'

3.2.1.5 FTP Support Procedures

3.2.1.5.1 Procedures to Resolve FTP1 Failures

Should the FTP1 Server fail, MCCs using FTP for alert data transmissions will have to be notified of the failure and requested to switch to the FTP2 Server address until the problem can be resolved. The following (**external**) FTP2 address is used for incoming and outbound traffic. The *password* is the same.

FTP**2** address: 140.90.241.11**6** (MCCs send to and receive from)

Note: The controller will have to notify CEMSCS (301- 457-5264) of the situation and ask them to change to the FTP**2** address until the problem can be resolved.

For outbound traffic.

a) Using CCI:

Remove the FTP server that COMM is monitoring by changing the field "Online" to [false] for all the MccFtp1 entries listed in table "ComFtpPathInCfg". The field "ServerPcName" contains the value "MccFtp1".

b) Using ComSiteDisplay:
Change the TypeSite "OverRide", Site "US_FtpRelay" to use:
FtpB: 192.168.4.116 (**internal address**)

c) Stop the MccFtp1 service: "OPS_FAXFTPRELAY" (if available)

d) Start the MccFtp2 service: "OPS_FAXFTPRELAY".

e) Re-Start the service: OPS_COMMPROCESS" (This reloads ComFtpPathInCfg).

3.2.1.5.2 Procedure for Trouble-shooting FTP Errors (MCCs and AFRCC)

a) Our Communication application: OPS_COMMPROCESS
When the send disposition status of our queued messages start turning into "**R**"s, for resolved-by-force, it is probable that our Communication service is hung.
ACTION:
Re-Start "**OPS_CommProcess**" from our communications machine (MccComm1/MccComm2)

b) Our Ftp Server: If OPS_CommProcess can not reach our Ftp server (MccFtp1/MccFtp2), the message will indicate a connection error and it will list the name of the site. Example:
USMCCFtpRelay (OUT) Ftp1: An attempt to send an FTP msg failed.
In this case, the site "USMCCFtpRelay" is our Ftp Server, to which Comm can not connect. To view the address of the attempted server, view all recent COMM messages within the range 3000-3999.
ACTION:
Re-Start the Mcc Ftp service OPS_FAXFTPRELAY on the MccFtp1 or MccFtp2 (depending on where we are sending ftp messages to be relayed.)
Log On as a local user:
i. Open the services control window.
ii. Highlight "OPS_FAXFTPRELAY" by selecting it.
iii. Stop and Start the service.
iv. Close the services window.

c) Our Ftp-Relay module. The symptoms are the same as above but one can clearly see that Comm is reaching the Ftp Server. Three messages should determine good comms to the server. These messages, 3701, 3707 and 3703, state: the Ftp server that comm is connecting to, the "*.tmp" file which is being created, and an indicator that a full connection/processing to the server was successful.
i. This scenario indicates that our Ftp Relay application is down.
ii. **ACTION:**
iii. Log On as a local user: (MccFtp1 or 2)

d) Open the services control window.

e) Highlight "OPS_FAXFTPRELAY" by selecting it.
f) Stop and Start the service.
g) Close the services window.

3.2.1.5.3 Procedure for trouble-shooting LUTFtp errors

FTP communication problems encountered while sending messages to **LUTs**

Determine the cause of the problem:

a) Our communication application being hung:
   When the send disposition status of our queued messages start turning into "**R**"s, for resolved-by-force, it is probable that our Communication service is hung.
   ACTION:
   Re-Start "**OPS_CommProcess**" from our communications machine (MccComm1/MccComm2)

b) Frame Relay Service:
   Send test messages to other LUTs that use FTP, to verify we have good Frame Relay service.

   If we have frame relay problems....
   ACTION:
   Open a trouble ticket with our Frame Relay Provider

c) LUT FTP Server down:
   ACTION:
   Log On as a local user: (LUTFtp1 or 2)
d) Open the services control window.
e) Highlight "LUTFtpRelay" by selecting it.
f) Stop and Start the service.
g) Close the services window.

FTP communication problems encountered while sending messages to **RCCs**

Determine the cause of the problem

a. Our Communication application: OPS_COMMPROCESS
   When the send disposition status of our queued messages start turning into "**R**"s, for resolved-by-force, it is probable that our Communication service is hung.
   ACTION:
   Re-Start "**OPS_CommProcess**" from our communications machine (MccComm1/MccComm2)

b. Our Ftp Server: If OPS_CommProcess can not reach our LUTFtp server (LUTFtp1/LUTFtp2), the message will indicate a connection error and it will list

the name of the site. Example:

LutFtpRelay (OUT) LUTFtp1: An attempt to send an FTP msg failed.
In this case, the site "LutFtpRelay" is our Ftp Server, to which Comm can not connect. To view the address of the attempted server, view all recent COMM messages within the range 3000-3999.

ACTION:

Log On as a local user: (LUTFtp1 or 2)

i. Open the services control window.
ii. Highlight "LUTFtpRelay" by selecting it.
iii. Stop and Start the service.
iv. Close the services window.

c. Our Ftp-Relay module. The symptoms are the same as above but one can clearly see that Comm is reaching the Ftp Server. Three messages should determine good comms to the server. These messages, 3701, 3707 and 3703, state: the Ftp server that comm is connecting to, the "*.tmp" file which is being created, and an indicator that a full connection/processing to the server was successful.

This scenario indicates that our Ftp Relay application is down.

ACTION:

Log On as a local user: (LUTFtp1 or 2)

i. Open the services control window.
ii. Highlight "LUTFtpRelay" by selecting it.
iii. Stop and Start the service.
iv. Close the services window.

3.2.2 Monitoring Procedures

The purpose of monitoring the operation of the USMCC is to ascertain that it is functioning properly. The primary method used to monitor operations is the "Scroll" program within the Operator Interface. As various processing activities take place within the USMCC, operator messages are displayed to the duty controller. Most of these messages simply reflect routine actions, for example, processing data from HI2 LUT. In order to distinguish between normal and abnormal conditions, each type of message has been assigned an "Operator Priority" (OP). Routine messages are assigned a low operator priority, but critical situations are awarded a higher priority. A high "OP" value is deemed to be a system alarm.

3.2.2.1 General Procedure for Alarms Handling

The Duty Controller will take action according to the operator message priority. The following criteria are to be applied:

Level I Alarm. This is the highest priority alarm. Any operator messages with an OP value between 45 and 49 inclusive are deemed to be a Level I alarm. These alarms represent fatal conditions that have disrupted operations and require immediate action. The controller must immediately inform his/her supervisor when this type of message is

received since outside assistance will likely be needed to restore operations. The controller shall also report all these alarms in the controller daily log. **SOP MCCOps05 provides further detailed procedures for handling Level I Alarms.**

Level II Alarm. This includes operator messages with OP values between 40 and 44. They represent potential problems that could develop into a Level 1 Alarm. These messages represent situations that have temporarily disrupted operations, but could become more serious. The controller must take immediate action to investigate the problem, but may be able to recover from the problem by following instructions provided for the alarm condition. During normal working hours, the Duty Controller shall notify his/her supervisor by telephone, or by email after hours. If unable to resolve the alarm condition, the alarm must be treated as a Level 1 alarm and the supervisor must be contacted. For example, "Pass from LUT xxx is late . . ". The delay may have been due to longer than normal LUT processing time, or temporary communications circuit problems, but the data was downloaded from the LUT either automatically or manually. Conversely, it may represent a more serious external problem with communications or the LUT. **Further procedures for Level II Alarms are provided in SOP MCCOps 06.**

Level III Alarm. Operator messages with OP values between 35 and 39 represent situations that are a potential problem and require further investigation by the duty controller. The controller shall undertake further investigation based on instructions provided for the specific alarm in order to verify the operational status. They may or may not escalate into more serious problems. For example, "Make sure that Alert is running .." could be because there has been no data to process recently. However, because it could also be due to a failure in the communication circuit between the USMCC and a LUT. Should it be determined that the operation has been degraded, the controller shall upgrade treatment as a Level II or Level I alarm. **SOP MCCOps07 covers procedures for Level III Alarms.**

Level IV Alarm. Operator messages with OP values between 30 and 34 are used to convey important information to the duty controller. They normally do not require further action. However, because the information is significant, they are presented in the message server box and require controller acknowledgement. For example, if a communication circuit is switched from the primary to the secondary circuit, a message is sent to the Controller confirming that the change has taken effect. **SOP MCCOps08 provides further guidance.**

Level V Alarm. Any operator message with an OP value less than 30 provides routine processing information and requires no action.

All operator messages that have a priority of 30 or higher are sent to a message server and displayed in a separate "pop up box". This box requires the controller to acknowledge the message. This box can be moved to different locations on the screen and will re-appear at the same location where it was last displayed. Controllers shall ensure that this box is kept at a location on the screen where its contents will be visible at

all times.

The time of acknowledgment and identification of the duty controller is automatically recorded. This information is recorded in the event that a supervisor needs to contact the person who was on duty at the time of the alarm in order to obtain further information concerning problems. The controller information is obtained from workstation login information. Therefore, if one controller is temporarily filling in when an alarm condition arises, it is important either to log on/off while filling in or to clearly record in the controller's log the name of the individual who responded to the alarm.

The USMCC software identifies a very large number of alarm conditions. However, some conditions represent external problems that invoke a different set of procedures. Instructions for handling specific, external alarms may be found in other SOPs and in the USMCC Operating Instructions document.

3.2.2.2 Procedures to Report Problems Encountered While Operating the USMCC.

If the problem is a critical problem that affects operations (i.e. alert processing, support to US RCCs, LUT scheduling and/or communications), call your supervisor. Log the problem and time that the call was made. The supervisor will provide additional on whether or not any specific data needs to be saved.
If operator screens are not producing expected results, or giving unusual errors:

a) Check that the correct database is selected (Connect on the menu bar).
b) Ensure that data entry matches required selections. For example, if a date-time box is checked, ensure that the times and dates are the desired values for your query, and not default time settings.
c) Verify that data is correctly entered in the correct format and that correctselections were made (i.e. output formatted for a message transmitted by the USMCC).

If the problem persists, make before and after copies of any screens, write down what you were trying to do, what happened, and why it appears to be a problem. Log the problem in the controllers daily log and leave a paper copy behind for your supervisor.

3.2.3 Controller Logging

The USMCC maintains a daily log of activity using the Controller Log Interface The log is used to record pertinent activities within the USMCC that are not captured automatically.

Procedures:
To access and use the USMCC Controller Daily Log:

a) OPS1 PC > start> Operator Interface> ControllerLog> Log On
b) Click on **Search/Refresh**
c) Select 'Single' or 'Multiple' lines radio button

d) Set up the different fields for comfort and readability by placing the cursor on the field division (column) lines and dragging the bar.
e) To make an entry into the Log, click on 'New Entry' in the Controller Log frame. There are multiple drop-down windows to select from that contain specific canned entries to speed up the process; otherwise you will have to compose your own entry.
f) In the case of Operator Alarm Messages, the alarm box contains an option to 'make a Log entry' which enters the message in the bottom half of the window, and the top half is used for a response to the message.
g) Log entries can be edited by clicking on the entry and selecting 'Edit Entry' in the Controller Log frame.
h) Searches can be conducted by selecting an 'Entry Type' and clicking **Search/Refresh,** or by selecting 'Msg String', entering a string, and clicking on **Search/Refresh**.
i) Viewing the log is controlled by the 'TimeBound' frame parameters; Start and Stop times are selectable.

The following events shall be recorded in the LOG:

i. All system reboots and down times, automatic and operator induced.
ii. All Site Query(s)..... OPlots and site status
iii. All SRR change requests
iv. All checks and tasks prompted by a timer
v. All calls for LUT/MCC support
vi. All anomalies
vii. All requests for missing messages to and from other MCCs
viii. All beacons entered in exception processing
ix. All System Configuration changes and System Action Notifications
x. All system communications problems and trouble ticket numbers
xi. All status changes or problems concerning COSPAS/SARSAT satellites
xii. The successful receipt, processing , and sending of COSPAS and SARSAT orbit vectors to the appropriate MCCs and LUTs.
xiii. The opening of the Morning Report for the new day
xiv. All counts concerning 406 registrations -- mailing, sorting, etc.
xv. All changes made to the system by Sam Baker, Joe Wagenhofer, Tom Griffin, and the programming (system action notifications) and operational staff.
xvi. 16) All telephone calls (received and made) that are relative to the daily operations of the USMCC.
xvii. All LUT communication checks, automatic or operator induced
xviii. All stop/start of processes or PCs..... Operational and Test systems
xix. All Alarm notification messages (pop-up window) are to be inserted into the LOG; indicate what action was taken and any results; use the "copy" button so the complete message will be logged.
xx. When logging RCC, MCC, and SPOC names in the Controller Log, please use the names from the ComSiteDisplay Interface. This will make the log entries more consistent and able to use a search string.

3.2.4 Daily Backup

USMCC data, documents and application software are backed up daily in case of a system failure.

Procedures:

Using Veritas BackupExec timers, three domains of the USMCC are backed up daily, DSD, DSDGov and MCC. Four separate jobs are run to backup these domains onto four separate tapes: a 10/20 GB tape for the DSD domain, a 20/40 GB tape for the DSDGov domain, a 20/40 GB tape for the MccDataBase SQLServer on the MCC domain and a 20/40 GB tape for other files on the MCC domain.

The tapes are stored in the tape cabinet in the USMCC Control Room. Each set contains 31 tapes, one for each day of the month. Each tape is labeled "XXX Day 1" through "XXX Day 31", where XXX is the Tape Label specified in the table below. For example, the backup tape for the DSDGov Domain for April 2 would be labeled "DSDGov Day 2".

All steps in the following procedure shall be performed by the Controller, unless noted otherwise.

For each of the four backups, a message is sent to the MccOps1 PC console requesting the proper tape be inserted, as noted in the table below. Retrieve the tape for the current GMT day from the tape cabinet and insert it into the tape drive of the PC to Perform the Backup.

Backup Begin Time	Item to Backup	Tape Label	PC to Perform the Backup
00:10z	MccDataBase SQLServer	MccSQL	MCCSecondary
01:10z	DSD Domain	DSD	MccBackup
01:15z	DSDGov Domain	DSDGov	DSDSecondary
01:20z	MCC Files (on MccProcess1, MccComm1, MccPrim)	MccFiles	MccFTP2

Table 1: Backup Schedule

a) If an error occurs **at the start** of a backup, then notify the Tape Backup Administrator immediately. If the Tape Backup Administrator is not available, then notify the Operations Supervisor immediately.

b) If an error occurs **after the successful start** of a backup, then notify the Tape

c) Backup Administrator and Operations Supervisor via email.

d) After each backup has finished, the tape will eject automatically and a status message will be sent to the MccOps1 PC console. Remove the tape from the tape drive.

e) Log all actions and status information in the Controllers Daily Log.

f) For the "MccSQL" and "DSD" tapes, remove the tapes currently in the Controller Emergency Evacuation Kit and place the new tapes in the Kit. If the *previous* day is not the first day of the month, then place the tapes for the previous day in the tape cabinet. If the *previous* day is the first day of the month, then re-label the tapes with the correct date (eg., "05/01/2002") and place them on the desk of the Tape Backup Courier.

g) For the "DSDGov" and "MccFiles" tapes, if the *current* day is not the first day of the month, then place the tapes in the tape cabinet. If it is the first day of the month, then re-label the tapes with the current date (eg., "05/01/2002") and place them on the desk of the Tape Backup Courier.

h) The Tape Backup Courier will deliver the "first day of the month" tapes to the offsite storage facility.

i) Once new tapes have been delivered to the offsite storage facility, the Tape Backup Courier will deliver the tapes from the previous month to the Tape Backup Administrator at the onsite facility. The Tape Backup Administrator will put the tapes into a safe box for permanent storage.

3.2.5 RCC Support

The prime mission of the USMCC is to support USA RCCs. A number of common scenarios that controllers will encounter are described below.

a) Forwarding Beacon information from MCCs to RCCs.
b) Request to change the Primary SRR for an active site
c) Request from an RCC for an OPLOT (Alert Site query).
d) Request from an RCC to reset their password for the online IHDB or RGDB.
e) Request from an RCC to close a 406 MHz alert site (Not allowed to close a 121.5/243 MHz site).

(Reference SOP RCC01 for further details on these activities)

3.2.6 LUT Support

3.2.6.1 Monitor and Resolve LUT Problems

Satellite passes that are scheduled by the USA LEOLUTs to be tracked shall be monitored by the Duty Controller in order to ensure that the ground system is functioning properly. This section describes actions to be undertaken when an anomaly is observed.

USA LEOLUTs gather and store data from Cospas-Sarsat satellites while they are being tracked. Once the satellite passes below the horizon (LUT LOS), the LUTs process the data then send the resulting solutions to the USMCC. Normally, a LUT completes this process within two minutes after LOS. Missing data is an indication of a possible LUT problem.

Transmission of data to and from the LUTs is via FTP over Sprint Frame Relay or FTP over dialed back-up line (PSTN). An attempt is made to send commands/data via Sprint Frame Relay, but if the attempt fails, an attempt (automatic switch is transparent) is made via a dial-out line; there are 8 lines available for dial-out to the LUTs (and one input line from the LUTs).

Reference SOP MCCLut01 for detailed procedures.

3.2.6.2 Send Orbit Vectors to the LUTs

Indications that a LUT has a problem with orbit vectors may be manifested by:

a) rejection of the USMCC schedule
b) operator message that a LUT has not acknowledged the vectors, or
c) LUT schedule does not match MCC schedule.

Also, if a LUT has been down for an extended period for maintenance, it may be necessary to manually send orbit vectors to that LUT.

New orbit vectors are scheduled to be sent to USA LUTs at 1210Z and 0010Z. If problems are observed around these times, the LUT may have been busy and did not process the incoming vectors. Thus the first action of the controller should take is to re-transmit the appropriate vectors to the faulty LUT(s).

If problems occur at other times of day (usually manifested by a schedule change), the USMCC calculates a set of orbit vectors at two hour intervals. In this situation, the controller shall transmit the set of orbit vectors that correspond to the next hourly interval. For example, if the problem is observed at 1930Z, the operator shall send the vector set that is valid at 2000Z.

3.2.6.3 Creation of LUT Pass Schedules

Pass Schedules are generated and sent to the U.S. LUTs daily. While the creation of LUT Pass Schedules is automated, manual intervention is sometimes required.

There are three main activities:

LUT pass schedule overview
Manually preparing the LUT pass schedules for transmission
Resending the LUT pass schedule

Reference SOP MCCLut04 for details

3.2.6.4 Changing LUT Data Destinations

On occasion it is necessary to change or to add an MCC destination for LUT data. This is accomplished in two major steps. First, a command is issued to the LUT to change or add a predefined MCC destination. This command may be issued at any time. Second, a command must be issued to cause the LUT to restart, in order for the change or add command to take effect. For a LEOLUT, the restart command should only be issued if the LUT is not taking a pass.

While the "Add" command adds an MCC destination to the current list of MCC destinations (with a maximum of 5 destinations), the "Change" command replaces the current list of MCC destinations with one destination. The list of active MCC destinations provides the destination(s) for all data that the LUT automatically generates, which includes LEOLUT pass data, GEOLUT solution data, LUT start up messages, and LUT status, warning and alarm messages. Note that the LUT will accept commands from any predefined MCC destination at any time, and send command responses solely to the MCC destination that issued the command.
Reference SOP MCCLut08 for further details

3.2.7 MCC Support

3.2.7.1 Support Information Requests from MCCs

a) **Request to continue to send data**
Data transmission to other MCCs normally terminates when ambiguity is resolved. However, situations will arise whereby an MCC may request the USMCC to continue to send data for a specific site. The following example shows how to respond to such a request:

> A composite site is active in the French AOR. FMCC has requested that data continue to be sent the FMCC after ambiguity resolution. Use the Operator Interface "Alert Site Query" screen to query by site number. Follow instructions in the USMCC Operating Instructions Manual to set the site to "Continue to send".

b) **Request for 406 Registration Information**

Receive call from an MCC requesting registration information for a USA beacon.

i. Access the 'SupportMessages' Interface
ii. Click on "406 RDB"
iii. Make a selection from the 'drop-down list' (first window in 'Registered BCN Search') by highlighting and clicking on "Beacon Id".
iv. Enter the beacon ID in the window directly below the 'drop-down list' window and click on the "Search" button .
v. The program will return the information if the vessel/aircraft/PLB is registered, otherwise it will return 'Beacon Not Found'.
vi. If the beacon is registered, it can be viewed (automatic) , edited, printed, and sent to the MCC.

To send the registration

i. Select the type of destination from the drop-down list of the first window in the' Send To:' section; MCC, RCC, or SPOC.
ii. 2) Select the destination from the drop-down list of the second window in the ' Send To:' section. "CMCC"
iii. 3) Operations selection ------ Click on Send to send the message.

c) **System Status Messages**

SIT 605, System Status messages, are used to notify other Cospas-Sarsat MCCs of any significant changes in the Cospas-Sarsat ground and space segments. Controllers will be notified of receipt of all incoming SIT 605 messages. Receipt of such messages shall be noted in the controller log. A copy of all incoming/outgoing SIT 605 messages shall be provided to the Chief, USMCC.

3.2.7.2 Identify and Correct Problems in the Daily Retrieval, Processing, and Sending of the Cospas-Sarsat Orbit Vectors

The USMCC extracts two line orbital elements for Cospas-Sarsat related satellites from the Naval Space Command Bulletin Board daily. Using the SGP4 model for "non-deep space" satellites, the USMCC verifies and propagates these orbital elements. The USMCC translates these elements into earth fixed orbit vectors (i.e., X, Y and Z positions and velocities) that are sent to U.S. LUTs and foreign MCCs. Orbit vectors are sent to LUTs regularly in order make Doppler locations as accurate as possible.

To determine if orbit vectors have been processed successfully and what to do if a problem occurs **refer to SOP MCCMcc02**.

3.2.7.3 Correct Problems with Processing of SARP Time Calibration

SARP Time Calibration (TCAL) data is used to provide calibration information for LUTs that track SARSAT satellites that have an operational Search And Rescue Processor (SARP). This information allows LUTs to translate on-board satellite time associated with a 406 MHz beacon message (and stored in the SARP) with Universal Time Coordinated (UTC) time used on the earth. The FMCC sends TCAL data (as a SIT 415

or 417) to other nodal MCCs early each Monday. TCAL data is sent in a SIT 415 for satellites without a SARP-3 processor. For satellites with a SARP-3 processor (that is, Sarsat-11 and higher), TCAL data is sent in a SIT 417.

When the USMCC receives TCAL data from the FMCC, the USMCC validates it, based on previous TCAL data per satellite. Once validated, the USMCC automatically distributes this data to USA LUTs and to other MCCs in the Western Data Distribution Region (DDR), the later is in accordance with the Cospas-Sarsat Data Distribution Plan (DDP C/S A.001).

Manual intervention is sometimes required to distribute TCAL data from the USMCC. The procedures to perform this intervention are detailed in **SOP MCCMcc03**.

3.2.7.4 Handling Problems with Receipt and Processing of Telemetry Data

The SARSAT space segment involves equipment from three different nations. Canada provides the instrumentation for the Search and Rescue Repeaters (SARR) and the downlink transmitter. France provides the instrumentation for the Search and Rescue Processor (SARP). The United States (NOAA) controls the satellite on which these instruments are carried and receives and processes telemetry information (data that monitors the health of these instruments).

As various SARSAT satellites are tracked, telemetry information is received at CEMSCS. CEMSCS sends telemetry information to the USMCC FTP server. (The USMCC FTP server is MCCFTP1 for the Operational system, MCCFTP2 for the Test system, and MCCFTP3 for the Offsite Backup system in Lanham). USMCC software transfers this information from the USMCC FTP server to appropriate SQL tables. The USMCC sends summary messages and out-of-limit messages to Canada and France for each satellite that has active instruments.

To resolve problems with the receipt and processing of SARSAT satellite telemetry data from CEMSCS **refer to the detailed procedures found in MCCMcc014**.

3.2.7.5 Backup Procedures

3.2.7.5.1 Procedures to Backup AUMCC

This procedure makes changes to configuration tables such that the USMCC assumes alert and system data distribution responsibilities for the AUMCC in the event that they request USMCC backup of the AUMCC Nodal responsibility.

Procedure:

From the OPS1 PC:

a. Start > OperatorInterface > CCI
b. Logon to CCI

i. Select the tab labeled “Message Routing/Formats”.
ii. (2) Within the frame labeled “Backup Procedures”, select the desired procedure from the “pull down” list..... **BackupAUMCCDo**
iii. Click on the “Run” button.

It should be noted that the “pull down” selection list (mentioned in Step 2) is dynamically generated with respect to which member of a given pair was last executed. Specifically, you will see either the “Do” or the “Undo” listed, but not both. Finally, it may be useful to mention that multiple configuration changes, and corresponding log entries, are actually associated with any one procedure. The number of configuration changes varies widely, ranging from only 2 up to more than 80.

c. When notification is received that AUMCC is assuming Nodal responsibility again, use the same procedure to ‘Undo’ the previous change..... **BackupAUMCCUndo**

d. All changes made are to be documented in the Controllers Daily Log.

3.2.7.5.2 Procedures to Backup CMCC

LUTs operated by the CMCC and USMCC provide overlapping coverage of each other’s areas of responsibility. Because much SAR activity occurs in border areas, there is frequent SAR coordination amongst RCCs in both areas, including Cospas-Sarsat alerts.

Procedure:
In the event of a failure at the CMCC, the USMCC is able to route data either via facsimile to the CMCC or to Canadian RCCs. The procedure used will depend upon the nature of the failure at the CMCC. If messages cannot be delivered to the CMCC automatically:

a. Contact the CMCC and determine the expected duration of the outage.
b. If the outages is expected to be short (less than one hour), use the communications interface to place CMCC messages on hold. Release the messages when
c. communications have been restored.
d. If and extended outage is expected, identify whether the CMCC wants Canadian alerts to be fax’ed to the CMCC or to Canadian RCCs. Configure communications paths accordingly.
e. Call your supervisor and brief on what’s happening.
f. When communications are restored, release any communications queues that have been placed on hold.
g. Log all actions and responses.

3.2.7.5.3 Procedures to Backup JAMCC

This procedure makes changes to configuration tables such that the USMCC assumes alert and system data distribution responsibilities for the JAMCC in the event that they request USMCC backup of the JAMCC Nodal responsibility.

Procedure:

i. Notify the Operations Supervisor.
ii. From the OPS1 PC:
iii. Start > OperatorInterface > CCI
iv. Logon to CC
    a) Select the tab labeled "Message Routing/Formats".
    b) Within the frame labeled "Backup Procedures", select the desired procedure from the "pull down" list..... **BackupJAMCCDo**
    c) Click on the "Run" button.

It should be noted that the "pull down" selection list (mentioned in Step 2) is dynamically generated with respect to which member of a given pair was last executed. Specifically, you will see either the "Do" or the "Undo" listed, but not both. Finally, it may be useful to mention that multiple configuration changes, and corresponding log entries, are actually associated with any one procedure. The number of configuration changes varies widely, ranging from only 2 up to more than 80.

h. When notification is received that JAMCC is assuming Nodal responsibility again, use the same procedure to 'Undo' the previous change..... **BackupJAMCCUndo**

i. All changes made are to be documented in the Controllers Daily Log.

3.2.7.5.4 Procedures to Implement When the SPMCC provides Backup for the FMCC

On occasion, the French MCC (FMCC) asks the Spanish MCC (SPMCC) to provide backup and assume Nodal responsibility for alert data distribution. In such an instance, the USMCC must redirect alert data to the Spanish MCC (SPMCC).

Procedure:

When notification is received from FMCC, via a SIT_605, that SPMCC will be providing backup and assuming Nodal responsibility until further notice, the USMCC Controller on duty must notify the Operations Supervisor and ask permission to redirect the alert data to SPMCC. This procedure makes changes to configuration tables to ensure that the USMCC properly distributes alert data to the SPMCC, as acting Nodal Backup for the FMCC. If permission is granted, proceed as follows:

From the OPS1 PC:

a. Start > OperatorInterface > CCI
b. Logon to CCI

i. Select the tab labeled “Message Routing/Formats”.
ii. Within the frame labeled “Backup Procedures”, select the desired procedure from the “pull down” list..... **SPMCCBackupFMCCDo**
iii. Click on the “Run” button.
iv. You will be prompted to confirm the action, and then to provide information for the Configuration Change Log.

It should be noted that the “pull down” selection list (mentioned in Step 2) is dynamically generated with respect to which member of a given pair was last executed. Specifically, you will see either the “Do” or the “Undo” listed, but not both. Finally, it may be useful to mention that multiple configuration changes, and corresponding log entries, are actually associated with any one procedure. The number of configuration changes varies widely, ranging from only 2 up to more than 80.

c. When notification is received that FMCC is assuming Nodal responsibility again, use the same procedure to ‘Undo’ the previous change..... **SPMCCBackupFMCCUndo**

d. All changes made are to be documented in the Controllers Daily Log.

3.2.7.5.5 Procedures to Implement the USMCC Backup

In the event of an actual or anticipated failure of the USMCC of over 4 hours, the AUMCC will assume the Nodal responsibilities and CMCC the National responsibilities. The AUMcc will distribute alert data, and System information, as appropriate, to MCCs in the Western DDR. AUMCC will also send alert data (intended for US RCC SRRs) to CMCC for distribution.

Procedures:

Notifying AUMCC and CMCC of USMCC operational failure:

a) When the USMCC determines they have serious operational problems that effect the ability to properly ingest, process, and distribute data (and cannot be resolved in the next four hours), personnel (Operations Supervisor or Duty Controller) will contact the AUMCC via telephone and request they assume USMCC nodal responsibilities, stating the reason for same. At the same time, a call will be placed to CMCC requesting they configure their system to support US National RCCs (Sit 185s to RCCs via email).

b) AUMCC and CMCC will provide an indication as to how long it will take to reconfigure for the backup role (this should normally be within the hour, depending upon availability of key personnel and time of day).

c) AUMCC will notify (via SIT 605) all MCCs of the problem, and their current role

and responsibilities. AUMCC will send alert data for US RCCs to CMCC for distribution, and FAX all alerts (SIT 185 format) for US SPOCs to (301) 568-8649. The USMCC will geosort the data and FAX to the appropriate SPOC(s).

d) CMCC will geosort alert data and send messages (via email) to the appropriate US RCCs using SIT 185 formats. Unlocated (GeoSar Alerts) will be sent to the USMCC email account 'usmcc@noaa.gov' in a SIT 965 format; the beacon will be checked for registration information (if the country code is in our RGDB) and then forwarded via fax to the appropriate RCC for prosecution or further distribution.

When the USMCC is ready to resume normal operations:

a) The On-Duty Controller shall contact the AUMCC and CMCC via a SIT 915 and coordinate the appropriate time for the USMCC to resume nodal and national responsibilities;
b) Contact the Western DDR MCCs and nodal MCCs by SIT 915 and advise them of the time the USMCC will resume nodal responsibilities; and
c) Advise all MCCs, using a SIT 605, that the USMCC is resuming normal operations as a nodal MCC, stating the time.
d) Advise all RCCs and SPOCs, using a SIT 950 and 915, that the USMCC is resuming normal operations as a nodal MCC, stating the time.

3.2.7.5.6 Procedures to Reroute Data from one MCC to Another MCC via the USMCC

This procedure defines the necessary configuration change when a request is made from an MCC for the USMCC to forward (reroute) their alert data to another MCC with whom communications have failed. If, for example, AUMCC cannot communicate with JAMCC and requests the USMCC to forward alert data to JAMCC, the SupportMccName in MccAlertRoutingCfg (for AUMCC) has to be changed from JAMCC to USMCC. This will work with all nodal MCCs that request our assistance.

Procedure:

e. Notify the Operations Supervisor.

From the OPS1 PC:

f. Start > OperatorInterface > CCI
g. Logon to CCI

(1) Select the tab labeled "Message Routing/Formats".
(2) Highlight and Left dbl click on "MccAlertRoutingCfg"

- Right dbl click on SourceMccName
- Click on 'Find Record'
- Enter name of source MCC
- Right dbl click on DestMccName
- Click on 'Find Record'
- Enter name of destination MCC
- Change the name of the supporting MCC to USMCC in SupportMccName date

(3) Notify the requesting MCC confirming the change has been made.
(4) All changes made are to be documented in the Controllers Daily Log.
(5) Follow the above procedure (reversing the MCC names in SupportMccName) to revert to normal distribution.

3.2.8 SPOC Support

Search and Rescue Points of Contact (SPOC) represent Search and Rescue authorities in countries that do not operate as a US RCC and do not operate MCC. They are destinations for Cospas-Sarsat alerts. There are three types of SPOCs:

Type 1 – alerts are sent directly to the SPOC from the USMCC

Type 2 - alerts are sent indirectly through COCESNA

Type 3 - the SPOC is normally served by another MCC.

Procedure:

For Type 1 SPOCs, direct communication with the SPOC is authorized and controllers may handle provide support similar to that provided USA RCCs.

Type 2 SPOCs represent Central American and countries. Requests for information are provided through COCESNA. The USMCC does not have automatic communications paths to these SPOCs.

Type 3 SPOCs should be handled via their host MCC. One exception is when the USMCC is serving as backup to the host MCC in which case they may be treated the same as Type 1 SPOCs.

SPOCs shall only be provided information regarding incidents within their own service area. Any other queries shall be treated as a Freedom of Information Access request.

3.2.9 Satellite Support

When a satellite payload is declared operational in the Cospas-Sarsat system, and whenever there is a change in the configuration or status of a satellite payload, the Space Segment Providers will notify all Ground Segment Operators. This information is provided in the message format described in C/S A.002, Figure II / F.1. This information should be incorporated into the USMCC configuration so that appropriate USMCC processing occurs.

See C/S document A.001 (DDP), Annex II / F for further information on the Status of Space Segment. See the Standard Operating Procedure (SOP) "CospasSarsatLaunch", as noted above, for information on enabling and disabling satellite processing.

When the USMCC receives a system message (SIT 605) concerning the Status of a Satellite, the Controller shall notify the Operations Supervisor, who will ensure that the procedure detailed in **SOP** MCCSat02 is followed.

3.2.10 Miscellaneous Support

3.2.10.1 Exception Processing

Tests that use 406 MHz beacons may be conducted in the United States or foreign countries. When tests are conducted that are associated with 406 MHz processing (eg., Cospas-Sarsat System Test, MCC or LUT Commissioning), it may be necessary to configure the USMCC software to process 406 MHz Beacon Ids specially. In order to accomplish this, the Configuration Control Interface (CCI) Operator Interface should be run for individual Beacon Ids or group of Beacon Ids, as outlined below. Once a test is completed, any configuration set up for the test should be removed or disabled.

The Beacon Test Coordinator should determine if special USMCC processing is required for a 406 MHz beacon, using the following table:

	Test Beacon	**Operational Beacon**
Special Distribution Required	Yes. Set Message Routing= Replace, SpecSRRs = to SRR(s) of distribution point(s)	Yes. Set Message Routing= Replace, SpecSRRs = to SRR(s) of distribution point(s)
Special Distribution Not Required	No	Yes. Set Message Routing= Replace, SpecSRRs = blank

Table 2: Special USMCC processing required by Beacon Type and Data Distribution Type (Changes reflect options provided in CCI *Operator Interface*)

Note that all Beacon Exception Processing updates cause changes to made to USMCC SQL table Alert124FilterCfg.
Refer to SOP MCCBcn04 for detailed procedures.

3.2.10.2 Monitoring the McMurdo Beacon

Given that Low Earth Orbiting (LEO) satellites are polar orbiting and that McMurdo Station is near the South Pole, it is expected that each LEO satellite with 406 MHz global capability will detect the McMurdo orbitography beacon on each pass. Consequently, it is expected that the U.S. LEOLUTs will detect the McMurdo orbitography beacon on each pass received from a LEO satellite with 406 MHz global capability. Accordingly, the USMCC (LMON service) monitors data received from the U.S. LEOLUTs to ensure that the 406 MHz orbitography beacon at McMurdo Station continues to transmit. **Refer to SOP MCCBcn05 for detailed instructions on how to respond to messages concerning the McMurdo beacon produced by LMON.**

3.2.10.3 Restarting the RGDB/IHDB

The USMCC Registration DataBase (RGDB) and the USMCC Incident History DataBase (IHDB) need to be available around the clock.

a) Notify the Operations Supervisor that the RGDB or IHDB is not responding and needs to be restarted.

b) To restart the RGDB:
   i. Log onto the APPSRV Computer
   ii. Click on Start> Settings>Control Panel>Administrative Tools> Services
   iii. Select “JRun NOAA Server”, and Click on “restart”.

-or-

   i. To restart the IHDB:
   ii. Log onto the RGDBWS1 Computer
   iii. Click on Start> Settings>Control Panel>Administrative Tools> Services
   iv. Select “JRun IHDB Server”, and Click on “restart”.

c) Log onto the WEBSRV Computer
   i. Click on Start> Settings>Control Panel>Administrative Tools> Services
   ii. Select “Apache2 Service”, and Click on “restart”.

d) If this does not resolve the problem, notify the Operations Supervisor.

e) Log off.

3.2.10.4 Updating Geosort

The Cospas-Sarsat Geosort Document defines the MCC Service Areas for alert data distribution. The boundary for each MCC Service Area, USMCC National RCC SRR, and USMCC SPOC, is defined by a totally enclosed set of individual latitude/longitude points. These points define a geosort region, which when queried by the USMCC

AlertProcess software program, returns an SRR code that is used to identify the alert message destination. The MapInfo COTS is used to manipulate the points and save them in a format for use by the USMCC AlertProcess software.
Refer to SOP MCCSrr01 for detailed procedures for updating SRRs.

3.2.10.5 Handling Beacon Testing Notifications from Foreign MCCs.

When a SIT 915 narrative (from a foreign MCC) "beacon test notification" is received at the USMCC, the Controller on duty is to:

1) Decode the beacon(s) for validation purposes.
2) Determine if special USMCC processing (exception processing) is required; if required, refer to Section 3.2.10.1, above.
3) Copy the narrative into the ControllerLog, (only if beacon has been entered into exception processing), Morning Report, and also enter in the Sarsat.Tests Oracle Calendar (MCCInternet PC).

Refer to SOP MCCTest03 for detailed instructions for calendar entry.

4.0 Use of the Remote Backup USMCC

In the case of a real emergency where the USMCC has to be evacuated, the Controller on duty is to **follow the detailed instructions in SOP MCC Sos02** If a decision is made to relocate to the USMCC Backup Site at Lanham, **use the detailed procedures provided in SOP MCCSos03** to resume control of the USMCC Operational System ***remotely***, **or**, if necessary, activate the system as ***operational*** from the Lanham facility located at: USMCC Lanham, Aerospace Building, 4th Floor, Room 452, 10210 Greenbelt Road Lanham, MD 20706

5.0 Glossary & Acronyms

Alert Message: Messages received from MCCs containing information to be acted on by Search and Rescue forces. (MCC SITs 100 - 199)

Archived Site: A Site in the USMCC which does not accept new data, and from which Alerts are not be issued.

AUMCC: Australia MCC

Beacon Pass: The passage of a beacon by a satellite. A beacon Pass is identified by the specific beacon, satellite, and TCA.

Beacon ID: Bits 26 - 85 in a coded 406-MHZ distress beacon.

CCI: Configuration Control Interface – software tool that provides automated reconfiguration in the USMCC to accommodate requirements for backing up other MCCs or allow special beacon processing.

CEMSCS: Central Environmental Satellite Computer System – NOAA computer system that provides SAR instrument telemetry data to the USMCC.

Closed Site: A Site in the USMCC into which incoming LUT or MCC data may be matched, but not merged, and from which Alerts are not be issued.

CMCC: Canada MCC

Composite Site: A Site with the ambiguity resolved and a composite location formed; the result of the Multiple Pass Merge or the Encoded Data Merge.

COTS: Commercial Off-The-Shelf

Default Beacon ID: Bits 26-85 in a coded 406 MHZ distress beacon with all bits that contain location set to default parameters as per Reference F for location protocol beacons.

DDP: Document produced and maintained by the Cospas-Sarsat Secretariat that describes the requirements for distributing data within the Cospas-Sarsat system. Also known as C/S A.001

ELT: Emergency Locator Transmitter

Encoded location: Location data contained in the National User Protocol, or the Standard or National Location Protocols, in 406-MHZ beacons, as given in Reference F.

EPIRB: Emergency Position Indicating Radio Beacon

FA: First Alert

FMCC: France MCC

FRD: Functional Requirements Document

FTP: File Transfer Protocol – communications protocol used to send and receive dataat the USMCC.

GEO: Geostationary Earth Orbiter

GEOLUT: LUTs that track and download data from SAR instrument-equipped GEO satellites.

Geosorting: The process of determining the Search and rescue Region for a given location on the Earth.

GMT: Greenwich Mean Time also known as UTC – Universal Time Coordinate.

IHDB: Incident History Data Base - a web-based repository for information on closed alert sites.

Incident Data: Data received from LUTs containing information on signals detected by COSPAS SARSAT satellites.

JMCC: Japan MCC

LEO: Low Earth Orbiter

LEOLUT: LUTs that track and download data from SAR instrument-equipped LEO satellites.

LMON: Software in the USMCC that monitors and reports on LUT activity.

LUT: US Local User Terminal – Ground Stations that track and download data from satellites equipped with Search and Rescue instruments

MCC: A Cospas-Sarsat Mission Control Center as listed in the C/S Data Distribution Plan

NESDIS: National Environmental Satellite, Data, and Information Service

NOAA: National Oceanic and Atmospheric Administration

NOCR: Notification of Country of Registration (SIT 133).

NSOF: NOAA Satellite Operations Facility – Facility on the Federal Office Complex in Suitland, Maryland that houses the USMCC, Maryland LUTs and the support staff.

RCC: Rescue Coordination Center

RGDB: Registration Data Base – a web based database that stores information on registration of 406 MHz beacons.

SA: Service Area

SAMS: Self-test And Monitoring System.

SAR: Search and Rescue

SARP: Search and Rescue Processor – Instrument aboard LEO satellites that receives and processes transmissions from 406 MHz beacons. The SARP stores data for continuous transmission to LUTs.

SARR: Search and Rescue Receiver - Instrument aboard LEO and GEO satellites that receives and processes transmissions from Cospas-Sarsat beacons.

SOG: System Operators Guide.

SOP: Standard Operating Procedure – a detailed description of how to perform a specific operations task for USMCC Controllers.

SPMCC: Spain MCC

SPOC: A SAR Point of Contact, as listed in the C/S Data Distribution Plan, Reference E, and contained in the USMCC GEOSORT Data Base.

SRR: Search and Rescue Region; the SAR Area designation returned by the GEOSORT for the relevant location is usually a SRR.

TCA: Time of closest approach of satellite to beacon.

TCAL: Time Calibration

USMCC: United States Mission Control Center

US SRR: A U. S. Coast Guard or US Air Force Rescue Coordination Center, as specified in the United States National Search and Rescue Plan, and contained in the GEOSORT Data Base.